PRIVACY AND CYBERSECURITY

ACT | The App Association and its members are committed to, and play a key role in, protecting end-user security and privacy. Our small to medium-sized members, operating across consumer verticals, recognise the ways in which the General Data Protection Regulation (GDPR) shapes privacy rights across Europe and beyond. The GDPR has not only set a global standard for data protection but also influenced privacy policies in other markets around the world.

IMPORTANCE OF PRIVACY AND CYBERSECURITY FOR SMALL APP COMPANIES

Our members care deeply about privacy, understanding that transparency and customer control over data collection and use are essential for building trust and fostering long-term relationships. Our members have made substantial investments to comply with GDPR, routinely going beyond its baseline requirements to meet both consumer expectations and competitive market pressures. This includes building in cutting-edge security and privacy features from the earliest stages of product development (privacy-by-design) and using advanced tools such as differential privacy techniques.

Both consumers and businesses need a pragmatic and scalable approach to privacy regulation. Small and medium-sized enterprises (SMEs) require the ability to appropriately tailor their approaches to the needs of their customers and partners, establishing and maintaining consumer confidence. Additionally, we advocate for the development of tools that can assist SMEs in implementing these regulations without compromising their ability to innovate and compete.

IMPACT OF REGULATORY ACTIONS

We are concerned about Member State laws and enforcement actions that may compromise privacy, creating an inconsistent regulatory environment across the EU. For example, the ePrivacy Directive, particularly concerning cookie regulations, has not met the expectations or needs of consumers or businesses. We welcome the European Commission's intent to withdraw the directive, as announced in its recent work programme.

Security threats in cyberspace present complex and quickly evolving policy challenges. We view the protection of users' personal information as a core responsibility and an opportunity for our members to earn consumer trust as a competitive advantage in the marketplace. That holds especially true when the personal information at issue involves the contents of users' sensitive communications or other sensitive information.

We believe that undermining encryption—such as mandating backdoors in encryption algorithms—cannot coexist with the principle of protecting users' personal information.

The initiatives related to cybersecurity such as digital sovereignty, the Child Sexual Abuse Directive, the Data Act, the European Health Data Space Act, and the Data Governance Act have significant implications for how data is managed and accessed within the EU. While each of these regulations is well intentioned, our members find the regulatory overlap to be difficult to navigate and harmful to consumer trust. It is essential that these initiatives protect privacy while allowing SMEs to operate and innovate freely in a global digital economy.

There are also regulations like the Digital Markets Act (DMA) that aren't directly related to privacy or cybersecurity but have sweeping impacts on the security of app ecosystems and consumer trust. We advocate for implementing the DMA in a way that preserves the ability of gatekeepers to protect the privacy and security in the app ecosystem by keeping out bad actors including untrustworthy alternative stores that may prey on consumer confusion. SMEs need an ecosystem that supports strong data and privacy protections and maintains robust cybersecurity measures.

EU policymakers must engage directly with SMEs to understand their operational challenges and strike a regulatory balance that protects consumer data and intellectual property while supporting small innovators' ability to scale and compete globally.